

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division**

IN RE: APPLICATION OF THE UNITED)	
STATES OF AMERICA FOR NON-)	
DISCLOSURE ORDER UNDER 18)	Case No. 1:25-DM-4 (WBP)
U.S.C. § 2705(b) RELATING TO)	
GRAND JURY SUBPOENA)	

MEMORANDUM OPINION AND ORDER

Before the Court are two applications submitted by the United States of America requesting non-disclosure orders (“NDOs”) under 18 U.S.C. § 2705(b) (“Applications”) to preclude two providers of electronic communication services (“Providers”) from notifying anyone—including their users, customers, or subscribers—of the existence of grand jury witness subpoenas 24-2/2024R00145-0004 and -0005 (“Grand Jury Subpoenas”) for a period of two years. After reviewing the Applications and the Grand Jury Subpoenas, the Court asked the government to address a question about the scope of the information requested from the Providers through the Grand Jury Subpoenas. When the government could not satisfactorily answer the Court’s question, declined to amend the scope of the Grand Jury Subpoenas, and challenged the Court’s authority to do anything other than enter the NDOs regardless of the scope of the Grand Jury Subpoenas, the Court declined to enter the NDOs, and the government asked for this order. Before drafting this order, the Court asked the government to outline its position in writing, which it has done (ECF No. 1; “USG Position”). The government’s submission raises two issues.

First, does the Court have discretion to refuse to enter an NDO precluding a provider of electronic communications services from notifying its customer about a grand jury subpoena if the Court believes that the government’s grand jury subpoena requests more information than

authorized by the Stored Communications Act? The government contends that the Court has no such discretion. For the reasons discussed below, the Court disagrees.

Second, does the Stored Communications Act allow the government to use a grand jury subpoena to request from a provider of electronic communications services “registration and session internet protocol (“IP”) addresses with associated port numbers,” a category of information not expressly authorized by 18 U.S.C. § 2703(c)(2)? For the reasons discussed below, the Court concludes that—while this information is not expressly described in Section 2703(c)(2)—it falls within the category of non-transactional basic subscriber information that may be obtained with a grand jury subpoena.

I.

A.

Putting aside for a moment the scope of the Grand Jury Subpoenas at issue here, the government first makes a broader, “jurisdiction[al]”¹ argument that a magistrate judge lacks discretion to refuse to enter an NDO authorized by 18 U.S.C. § 2705(b) if he believes the government’s grand jury subpoena exceeds that permitted by the Stored Communications Act. (ECF No. 1 at 1.) Instead, argues the government, regardless of whether its request seeks information prohibited by the Stored Communications Act, the Court must none-the-less give its imprimatur to a grand jury subpoena that—on its face—exceeds the law by allowing the government to attach to it an NDO signed by a federal judge. (*Id.* at 1-2.) According to the government, any review by the Court of the grand jury subpoena for compliance with the Stored Communication Act amounts to an “advisory opinion.” (ECF No. 1 at 1.) Instead, the

¹ There can be no doubt in this district that a magistrate judge has jurisdiction to evaluate NDOs and subpoenas submitted by the government for service on providers under the Stored Communications Act. *See* 28 U.S.C. § 636 and E.D. VA. LOC. CRIM. R. 5.

government argues that the Court may do nothing more than evaluate whether providing notice of the subpoena to a provider's subscriber might cause one of the five adverse results outlined in 18 U.S.C. § 2705(b) (e.g., risk of flight, destruction of evidence). (ECF No. 1 at 2.) The government leaves to the provider the "sole responsibility to challenge a grand jury subpoena at the outset." (*Id.*) Of course, the provider does not get to participate in the process "at the outset," and when a challenge is made, it is made to the restrictions imposed by the Court through the NDO, not simply to the scope of the grand jury subpoena. For these reasons and those described below, the Court rejects the government's "jurisdictional" argument.

B.

The Stored Communications Act ("SCA"), enacted as Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), protects the privacy of stored electronic files held by providers about their users, customers, and subscribers²; outlines how the government may access this data; and in some cases requires the government to notify a subscriber that it has requested their information. *See* 18 U.S.C. §§ 2701-2713. Within the SCA, Section 2703 regulates the different ways the government can obtain from a subscriber's electronic communications and other information, as well as the different levels of privacy protection afforded the subscriber, depending on the type of information requested by the government (i.e., content or non-content), and how the government chooses to request it (e.g., warrant, court order, or subpoena). 18 U.S.C. § 2703(a)-(c).

² The terms "user," "customer," and "subscriber" are technically distinct under the SCA, but the distinction is immaterial to the issue here. The Court therefore uses them interchangeably. *In re Application of the U.S. for an Ord. Pursuant to 18 U.S.C. sec. 2703(d)*, 830 F. Supp. 2d 114, 118 (E.D. Va. 2011).

The government may obtain the *content* of a subscriber’s communications from a provider using a warrant, an administrative subpoena, a grand jury subpoena, a trial subpoena, or a court order, but only if the government follows the procedures and notice requirements outlined in Section 2703(b)(1). *See* 18 U.S.C. § 2703(b)(1)(A)–(B). If the government uses a subpoena or a court order to obtain the content of communications, it must provide prior notice to the subscriber, although this notice to the subscriber may be delayed for no more than 90 days. *See* 18 U.S.C. §§ 2703(b)(1)(B) and 2705(a)(1)(A) and (B). If the government uses a warrant to obtain the content of a subscriber’s communications, it need not provide any notice to the subscriber. 18 U.S.C. § 2703(b)(1)(A).

If, as here, the government requests *non-content* “record[s] or other information pertaining to a subscriber” (“Subscriber Information”), it must follow the procedures outlined in Section 2703(c)(1). Like Section 2703(b)(1), the scope of the non-content records the government may obtain from a provider about a subscriber depends on the discovery device used and the showing the government must make to obtain it. If the government wants all non-content Subscriber Information, it must either (1) obtain a warrant from the court based on a showing of probable cause as required by Rule 41 of the Federal Rules of Criminal Procedure, (2) obtain a court order based on a showing of specific and articulable facts that the Subscriber Information is relevant and material to an ongoing criminal investigation under 18 U.S.C. § 2703(d), or (3) obtain the consent of the provider’s subscriber.³ 18 U.S.C. § 2703(c)(1)(A)–(C).

Section 2703(c)(1) also allows the government to issue an administrative or grand jury subpoena (collectively, “subpoena”). While the government can issue a subpoena to a provider

³ One other procedure exists under Section 2703(c) that relates specifically to telemarketing fraud, which is irrelevant here. *See* 18 U.S.C. § 2703(c)(1)(D).

without any prior court review or approval, the statute restricts the information the government can obtain about a subscriber to a smaller subcategory of non-content Subscriber Information, often referred to as “Basic Subscriber Information.” See *United States v. Taylor*, 54 F.4th 795, 804 (4th Cir. 2022). Specifically, Section 2703(c)(1)(E) and (c)(2) allow the government to obtain with a subpoena only the following Basic Subscriber Information about a subscriber:

(A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of services utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number).

18 U.S.C. § 2703(c)(2).

Unlike a request for content information under Section 2703(b)(1), the government has no obligation to notify a subscriber that it has requested this non-content Subscriber or Basic Subscriber Information. 18 U.S.C. § 2703(c)(3) (“A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.”).

In sum, Section 2703 creates a sliding scale that balances the type of information the government can obtain, the showing the government must make to obtain it, the subscriber’s privacy rights to the information, and the notice (if any) that must be provided by the government to the subscriber.

C.

Regardless of any obligation the SCA imposes on the government to notify a subscriber that the government has requested their electronic information, providers often contractually obligate themselves—or voluntarily assume the obligation—to notify their subscribers that the government has requested their information. And it does not matter if the government requested the subscriber’s information with a grand jury subpoena because Rule 6(e)(2) of the Federal

Rules of Criminal Procedure imposes no duty of secrecy on the recipient of a grand jury subpoena. *See* FED. R. CRIM. P. 6(e)(2) (“No obligation of secrecy may be imposed on any person except in accordance with Rule 6(e)(2)(B),” and the recipient of a grand jury subpoena is not one of them.).

Limiting the discussion here to the government’s ability to prevent a provider from notifying its subscriber that the government has issued a subpoena for the subscriber’s Basic Subscriber Information, 18 U.S.C. § 2705(b) allows the government to ask the court to issue an NDO to a provider if the government can show that disclosure to the subscriber will result in an adverse result. As applied here, Section 2705(b) states as follows:

(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS. —A governmental entity *acting under section 2703*, . . . may apply to a court for an order commanding a [provider] to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in [adverse results].

18 U.S.C. 2705(b) (emphasis added).

Therefore, if the government has no obligation to provide notice to a subscriber about a subpoena but believes that some adverse result will occur if a provider tells its subscriber about the subpoena, the government may ask the court to enter an NDO that prohibits the provider from notifying its subscriber about the subpoena.

D.

Turning to the first issue addressed by this order, the government argues that, when it applies for an NDO to accompany a grand jury subpoena, “[t]he Court must limit its consideration to the sole issue before it: the application for non-disclosure orders.” (USG Position at 1.) The government continues, “[a]s set forth in 18 U.S.C. § 2705(b), the Magistrate

Judge's review of an application for a [NDO] is therefore limited to whether 'there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in' one of the five listed adverse results." (ECF No. 1 at 2.)

The government reads Section 2705(b) too narrowly and overlooks the section's threshold requirement: the government may only request an NDO if it is "*acting under section 2703.*" 18 U.S.C. § 2703(b) (emphasis added). As discussed above, Section 2703 creates a sliding scale that balances the type of information the government can obtain, the required showing that must be made for each discovery device, the subscriber's privacy rights, and the notice (if any) that must be provided by the government to the subscriber. *See supra* Section I.B. Therefore, as a condition to ask the court for an NDO, the government must engage in discovery permitted by Section 2703.

If the government wants non-content Subscriber Information, it must either (1) obtain a warrant from the court as required by Rule 41 of the Federal Rules of Criminal Procedure based on a showing of probable cause, (2) obtain a court order under 18 U.S.C. § 2703(d) based on a showing of specific and articulable facts that the Subscriber Information is relevant and material to an ongoing criminal investigation, or (3) obtain the subscriber's consent. 18 U.S.C. § 2703(c)(1)(A)-(C). If the government wants to use a subpoena to obtain non-content Subscriber Information about a subscriber, the government must either have the subscriber's consent, 18 U.S.C. § 2703(b)(1)(B)(i), or it must limit its request to the Basic Subscriber Information permitted by Section 2703(c)(2). Without satisfying one of the above requirements, the government is not "acting under Section 2703," and a magistrate judge must not enter an NDO authorized by Section 2705(b).

If, for example, the government issues a grand jury subpoena to a provider demanding the content of a subscriber's communications without the subscriber's consent—information that may be obtained only with a warrant—the Court is not obligated to enter an NDO prohibiting the provider from disclosing the existence of the subpoena to the subscriber simply because the government has made a factual showing of a possible adverse result. Why? Because in such a hypothetical situation, the government is not “acting under section 2703” as that statute does not allow the government to obtain content information with a subpoena without the subscriber's consent, and thus a magistrate judge must not enter such an NDO to the provider. *See* 18 U.S.C. §§ 2703(b)(1)(B)(i) and 2703(c)(1)(C).

Similarly, if the government wants to obtain non-content information about a subscriber with a subpoena and without the subscriber's consent, and the government also wants to prohibit the provider from notifying its subscriber about the subpoena—to be “acting under section 2703,” and thus eligible for an NDO—the government must limit its request to the Basic Subscriber Information specifically permitted by Section 2703(c)(2). *See* 18 U.S.C. §§ 2703(c)(1)(C) and (c)(2).

None of this is to say that the Court can prevent the government from issuing grand jury subpoenas as it sees fit (and at its own peril). But when the government asks the Court to enter an NDO authorized by Section 2705(d), its request for discovery must comply with Section 2703. In this way, Congress has seen fit to vest the Court with the authority to ensure that the government's request complies with the law. If, as the government suggests, such judicial review is not required, the Court would be betraying the long-established system of checks and balances attendant to the *ex parte* discovery process in criminal cases before a person's private information is disclosed to the government.

For these reasons, before a magistrate judge enters an NDO as authorized by Section 2705(b), in the undersigned’s opinion, the judge must review the subpoena to determine whether the government has complied with Section 2703.

II.

A.

This kerfuffle began when the Court asked the government to answer a simple question: what are “registration and session IP addresses with associated port numbers,” and how do they relate to the Basic Subscriber Information permitted by Section 2703(c)(2). The question arose from the Court’s review of the government’s Applications for NDOs relating to the Grand Jury Subpoenas. The Court raised the question because—more and more—it has seen the government request NDOs from the Court that prohibit providers from notifying their subscribers about subpoenas that ask for more information than is expressly permitted by Section 2703(c)(2). In the Court’s view, and as discussed above (Section I.D.), if the government applies for an NDO to prohibit a provider from informing its subscriber about a subpoena from the government, the government is limited to requesting the specific information described in Section 2703(c)(1), i.e., Basic Subscriber Information.

While the list of Basic Subscriber Information purports to be exhaustive, the SCA was adopted in 1986, and technological advancements—at least in the eyes of the government—have changed the types of information that should be considered Basic Subscriber Information. This scenario has presented itself to this Court in many ways, the most common of which—and the one at issue—involves the government requesting the specific information outlined in Section 2703(c)(2) but then adding parenthetical information that is not obviously related to the statutory item. Here, after requesting “other subscriber numbers or identities, including any temporarily

assigned network addresses,” a category of information expressly permitted by Section 2703(c)(2)(E), the government added the parenthetical “(including the registration and session IP addresses with associated port numbers).” (Grand Jury Subpoenas, Attachment A.)

When the Court could not get a satisfactory answer to its question—what are these things and how do they relate to Basic Subscriber Information?—it refused to enter the NDOs for the Grand Jury Subpoenas, and the government asked for this order. Having now conducted its own research, the Court concludes that “registration and session IP addresses with associated port numbers” amount to non-transactional information that fall within the categories of “telephone connection records, or records of session times and durations” and “instrument number[s] or other subscriber number[s] or identit[ies], including any temporarily assigned network address[es]” and therefore will approve the NDOs. In any event, having taken the time to research the issue and concluding that there may be others who do not know what a “port number” is or how it fits within the scope of Basic Subscriber Information authorized by Section 2703(c)(2), the Court summarizes its research below.

B.

Congress created the Stored Communications Act in response to “tremendous advances in telecommunications and computer technologies,” which led to technological advances in surveillance. S. REP. 99-541, at 3 (1986). Congress was concerned that technological advances in surveillance could lead to overzealous law enforcement agencies obtaining personal and business information that they were not privy to before. *See id.* Created in the aftermath of *United States v. Miller*, 425 U.S. 435 (1976)—where the Supreme Court held that a bank customer lacked standing to contest the disclosure of his bank records to the government—

Congress sought to protect third party information kept on computers because “computers are used extensively . . . for the storage and processing of information.” S. REP. 99-541, at 3 (1986).

Prior to the 1994 Amendments to the SCA, Congress did not distinguish between Basic Subscriber Information and other information relating to a subscriber. *Id.* Rather, law enforcement was allowed to use an administrative or grand jury subpoena to generally obtain “information pertaining to subscriber or customer, but not the contents of any communications of that customer.” *Id.*

By the 1990s, Congress recognized that, “in the eight years since the enactment of the [Electronic Communications Privacy Act], society’s patterns of using electronic communications technologies ha[d] changed drastically.” H.R. REP. 103-827, at 17 (1994). Because individuals maintained “a wide range of relationships” online, Congress decided that *transactional data*—such as email addresses and websites visited—that document an individual’s online activities and associations reveals a great deal of information about an online-user’s private life, and Congress did not want law enforcement to obtain this type of transactional data with simply a subpoena. *See id.* Thus, to “guard against ‘fishing expeditions’ by law enforcement,” Congress amended the SCA in 1994 to, among other things, distinguish between Basic Subscriber Information, which could be obtained using a subpoena, and “other information pertaining to a subscriber”—including non-content, transactional data—which required a court order. H.R. REP. 103-827, at 10 and 17 (1994) (“In addition, the bill increases the protection for transactional data on electronic communications services by requiring law enforcement to obtain a court order for access to electronic mail addressing information.”).

The SCA now itemizes in 18 U.S.C. § 2703(c)(2) the Basic Subscriber Information that law enforcement can obtain from a provider with a subpoena. Basic subscriber records include a

customer's name and address; telephone call records, including the time and duration of calls; length of service including the start date for the account and types of service provided; telephone number or other subscriber number or identity, including temporarily assigned network addresses; and method of payment, including credit card or bank account numbers. 18 U.S.C. § 2703(c)(2). Basic Subscriber Information does not include a customer's transactional data, such as addresses of websites visited by the customer and email addresses of other individuals with whom the account holder has corresponded.

Today, the broader term "other information pertaining to a subscriber," 18 U.S.C. § 2703(c), includes transactional records, such as logs recording account usage, the email addresses of individuals with whom the customer has corresponded, and the websites a customer has visited, and this information may be obtained only by a court order after showing "specific and articulable facts showing that there are reasonable grounds to believe" that the records requested are "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

* * *

The question for the Court, then, is whether "registration and session IP addresses with associated port numbers" constitute non-transactional Basic Subscriber Information that may be obtained by the government with a subpoena or whether it is transactional "other information pertaining to a subscriber" for which the government needs a court order.

C.

An internet protocol address is a "unique numerical figure that identifies an electronic device accessing the Internet, and it is used to route information between Internet-connected devices." *United States v. Sanders*, 107 F.4th 234, 241 n.2 (4th Cir. 2024). Computers communicate with each other through "IP packets." See *Trend Micro Inc. v. CUPP Computing*

AS, No. 2020-2237, 2022 WL 14366176, at *1 (Fed. Cir. Oct. 25, 2022). These packets include source IP addresses and destination IP addresses, which are used to identify source and destination computers. An IP packet may also include “source and destination port numbers to identify source and destination *applications* within the source and destination computers.” *Id.* (emphasis added.) According to the Federal Circuit, “IP addresses and port numbers are important for reliably communicating, by initial message and reply, between the source and intended destination.” *Id.*

Courts have held that individuals do not have a reasonable expectation of privacy in their IP addresses. *See United States v. Orisakwe*, 624 F. App’x 149, 155 (5th Cir. 2015). According to the Ninth Circuit, this because internet users “should know that [IP addresses and basic subscriber information] are provided to and used by Internet service providers for the specific purpose of directing the routing of information.” *United States v. Rosenow*, 50 F.4th 715, 738 (9th Cir. 2022).

The government points out in its papers that a “[n]otabl[e]” distinction about its request is that it seeks only *session* IP addresses, not *transactional* IP addresses, which provide “more extensive information.” (ECF No. 1 at 3-4.) The government then argues, essentially, that providers understand the distinction between the two types of IP addresses and have internal procedures allowing the government to obtain *session* IP addresses by subpoena and *transactional* IP addresses by court order. (*Id.* at 4.)

While the government provides no research or substantive discussion on the difference between session and transactional IP addresses, open-source research shows that a “session IP address” refers to the IP address used to identify a user’s ongoing interaction with a network and is analogous to source and destination telephone numbers. Session IP addresses are assigned to

users when they connect to a network, so the network knows who (source IP) sent a particular piece of data to whom (destination IP). A “transactional IP address” is used to identify the specific IP address involved in a particular request or action, such as an online purchase or the submission of a form.

The Court also turned to open-source research to understand “port numbers.” The best description of port numbers and how they relate to IP addresses the Court could find, is as follows:

An IP address identifies a machine in an IP network and is used to determine the destination of a data packet. Port numbers identify a particular application or service on a system. As an analogy, if each computer were a building and the internet were a city, then the IP address would be the building’s street address, and the port number would be the apartment number.

An IP address is a logical address used to identify a device on the network. Any device connected to the internet or network is assigned a unique IP address for identification. This identifying information enables devices to communicate over the internet.

Port numbers are part of the addressing information that helps identify senders and receivers of information and a particular application on the devices.

Gavin Wright, *What Are Port Numbers and How Do They Work?*, TECHTARGET (March 2025), <https://www.techtargert.com/searchnetworking/definition/port-number#:~:text=As%20an%20analogy%2C%20if%20each,a%20device%20on%20the%20network>. So, port number data helps to identify a specific application or service on the internet or a network, enabling communication, but it does not contain the actual data exchanged during a transaction.

Based on the above, a request for session IP addresses and associated port numbers would seem to produce the dates and times a user connected to a network and the applications or services on the internet or network involved in the transmission. This is distinct from a request

for transactional information, such as the addresses of websites visited by the customer and email addresses of other individuals with whom the account holder has corresponded.


A request for session IP addresses and associated port numbers will not disclose transactional information, but it is like a request for “telephone connection, or records of session times and durations” and “telephone or instrument numbers or other subscriber number or identity, including any temporarily assigned network addresses,” both of which are expressly authorized by 18 U.S.C. § 2703(c)(2). The Court finds therefore that the government’s request for “session IP addresses and associated port numbers” constitutes non-transactional Basic Subscriber Information that may be obtained by the government with a subpoena.

IV.

Should the government still wish for the Court to enter the NDOs for the Grand Jury Subpoenas, it may submit them to the Court with updated dates, and the Court will promptly enter them.

Entered this 9th day of April 2025.

Alexandria, Virginia



William B. Porter
United States Magistrate Judge